[redacted]

From: [redacted]
Sent: Sunday, June 08, 2014 4:54 PM
To: [redacted]
Subject: Data Security Breach Notification - College of the Desert

Categories: Orange Category

Data Security Breach Notification

To: College of the Desert Colleague

From: Department of Human Resources and Labor Relations, College of the Desert

Date: June 8, 2014

Re: Notification of Data Security Breach Affecting or Potentially Affecting the Security of Your Personal Information

This notice is to inform you that your personal information was affected or potentially was affected by a recent data security breach at the College of the Desert. The College seeks to protect you and your personal information. The College has already taken steps to mitigate the impact of this data security breach and protect you and your personal information going forward.

The College of the Desert, located at 43-500 Monterey Avenue, Palm Desert, CA 92260, experienced a data security breach on Thursday, June 5, 2014. The data security breach involved the release of the following types of your personal information: your name, social security number, date of birth, gender, home zip code, the titles of positions you held at the College (including start and end date of each position held), your employment anniversary date, employee identification number, health insurance benefit plan selection, health insurance subscriber identification number, amount or cost of health insurance subscriber premium, and active or retired employee status.

The breach incident occurred in the afternoon on Thursday, June 5, 2014. A College employee, without authorization, sent an electronic mail message with an attached spreadsheet containing the above classes of personal information. This e-mail message was sent to a group of approximately 78 College employees. A message recall was attempted and was successful with some but not all recipients. That recall was done less than an hour after the email was sent. However, it is possible that the e-mail and its attached spreadsheet was delivered to approximately fifty people, all of whom are employees of the college. We cannot determine how many people actually opened the email or viewed the attachment. We can assure you that the email was, within less than 24 hours, removed from everyone's mail box and deleted. The College has already taken some steps to mitigate the impact of this breach. All recipients have been directed not to open, print, or save the contents of the message, including its attachment, and they have also been instructed to delete the message with its attachment. Those email recipients will again be reminded not to disclose any information contained in the email. These measures appear to have been partially successful at limiting the disclosure of your personal information to unintended recipients.

In addition, the College is working with its IT personnel to pinpoint precisely where and to whom personal information was inappropriately disclosed, as well as examining additional security protocols and procedures for

the protection of personal information. The College will continue to take additional precautions to limit the exposure of your personal information.

This notification has been sent at the earliest time possible and was not delayed as a result of a law enforcement investigation or otherwise. Investigations shall continue, as necessary, to ensure future data security breaches are avoided.

To verify the security of your personal information or to take additional steps to protect yourself, the major credit reporting agencies may be contacted at the following toll-free telephone numbers and addresses:

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111

Experian (www.experian.com)
P.O. Box 2104
Allen, TX 75013-0949
1-888-EXPERIAN (397-3742)

Trans Union (www.transunion.com)
P.O. Box 1000
Chester, PA 19022
1-800-916-8800

I am attaching an article from the state's Attorney General's Office which contains some helpful information regarding actions you can take when you believe your personal & confidential information may have been viewed by others. The website for the article is http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/CIS_3_victim_checklist_DOJ.pdf. Each of the above three credit agencies offers a service (most commonly referred to as a "Fraud Alert") whereby any time any person or entity takes any action that could affect your credit you are immediately notified. The College will reimburse you for the reasonable cost of that service for one year.

Please do not hesitate to contact the College of the Desert to discuss the data security breach and the security of your personal information. Please direct inquiries to Human Resources and Labor Relations Executive Director Stan Dupree. Mr. Dupree may be contacted at (760) 674-3777 or sdupree@collegeofthedesert.edu. The College of the Desert apologizes for any inconvenience this data security breach may cause and looks forward to correcting this breach in the most expedient fashion to increase the security of your personal information.

You will receive a copy of this letter via email and by regular mail.

IDENTITY THEFT VICTIM CHECKLIST

This checklist can help identity theft victims clear up their records. It lists the actions most identity theft victims should take to limit the damage done by the thief. For more information, see the Web sites of the Federal Trade Commission atwww.ftc.gov/idtheft, the Identity Theft Resource Center at www.idtheftcenter.org, and the Privacy Rights Clearinghouse atwww.privacyrights.org

Report the Fraud to the Three Major Credit Bureaus

You can report the identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system and you will not be able to speak to anyone at this time. The system will ask you to enter your Social Security number and other information to identify yourself. The automated system allows you to flag your file with a fraud alert at all three bureaus. This helps stop a thief from opening new accounts in your name. The alert stays on for 90 days. Each of the credit bureaus will send you a letter confirming your fraud alert and giving instructions on how to get a copy of your credit report. As a victim of identity theft, you will not be charged for these reports. Each report you receive will contain a telephone number you can call to speak to someone in the credit bureau's fraud department.

Experian 1-888-397-3742

experian.com/fraud/center.html

Equifax 1-800-525-6285

alerts.equifax.com

TransUnion 1-800-680-7289

transunion.com

Report the Crime to the Police

Under California law, you can report identity theft to your local police department.[1] Ask the police to issue a police report of identity theft. Give the police as much information on the theft as possible. One way to do this is to provide copies of your credit reports showing the items related to identity theft. Black out other items not related to identity theft. Give the police any new evidence you collect to add to your report. Be sure to get a copy of your police report. You will need to give copies to creditors and the credit bureaus. For more information, see "Organizing Your Identity Theft Case" by the the Identity Theft Resource Center, available at http://www.idtheftcenter.org/Fact-Sheets/fs106.html.

Request Information on Fraudulent Accounts

When you file your police report of identity theft, the officer may give you forms to use to request account information from credit grantors, utilities or cell phone service companies. If the officer does not do this, you can use the form in our Consumer Information Sheet 3A: Requesting Information on Fraudulent Accounts. When you write to creditors where the thief opened or applied for accounts, send copies of the forms, along with copies of the police report. Give the information you receive from creditors to the officer investigating your case.

Call Creditors

Call creditors for any accounts that the thief opened or used. When you call, ask for the security or fraud department. Examples of creditors are credit card companies, other lenders, phone companies, other utility companies, and department stores. Tell them you are an identity theft victim. Ask them not to hold you responsible for new accounts opened by the thief.

If your existing credit accounts have been used fraudulently, ask the credit issuers to close those accounts and to report them to credit bureaus as "closed at consumer's request." If you open a new account, have it set up to require a password or PIN to approve use. Don't use your mother's maiden name or the last four numbers of your Social Security number as your password.

Ask the creditors to give you copies of documentation on the fraudulent accounts (see above item). For more information on what to tell creditors, see the Federal Trade Commission's identity theft Web site atwww.consumer.gov/idtheft

Review Your Credit Reports Carefully

When you receive your credit reports, read them carefully. Look for accounts you don't recognize. Look in the inquiries section for names of creditors from whom you haven't requested credit. You may find some inquiries identified as "promotional." These occur when a company has gotten your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (By calling to report identity theft, your name will be automatically removed from the mailing list to receive unsolicited credit offers of this kind.) Also, as a general precaution, look in the personal information section to verify your Social Security number, address and name.

If you find anything you don't understand, call the credit bureau at the telephone number listed on the report. Tell them you want to block, or remove, any information on the report that is the result of identity theft. (You must send a police report of identity theft to support this request.) For more on what to tell the credit bureaus, see the Privacy Rights Clearinghouse's "Identity Theft: What to Do When It Happens to You" www.privacyrights.org/fs/fs17a.htm

Use the ID Theft Affidavit

Creditors may ask you to fill out fraud affidavits. The Federal Trade Commission's ID Theft Affidavit is accepted by the credit bureaus and by most major creditors. Send copies of the completed form to creditors where the thief opened accounts in your name. Also send copies to creditors where the thief made charges on your account, to the credit bureaus, and to the police. The form is available on the FTC Web site at ww.ftc.gov/bcp/edu/resources/forms/affidavit.pdf. File a complaint of identity theft with the FTC. See their Web site at www.consumer.gov/idtheft The FTC keeps a database of identity theft cases that is used by many law enforcement agencies.

Write to the Credit Bureaus

Write a letter to each credit bureau. Repeat what you said in your telephone call (see above). Send copies of your police report and completed ID Theft Affidavit. Remind the credit bureaus that they must block or remove any information that you, as an identity theft victim, say is a result of the theft. Send your letters by certified mail, return receipt requested. Keep a copy of each letter. See the Sample Letter to Credit Bureaus on page 7.

Equifax

P.O Box 740241

Atlanta, GA 30374-024

Experian

P.O. Box 9532

Allen, TX 75013

TransUnion

P.O. Box 6790

Fullerton, CA 92834

As an alternative, you may dispute items with the credit bureaus online. Look for "dispute" on their websites:equifax.com/home/en_us, experian.com, and transunion.com.

Request Additional Free Credit Reports

California identity theft victims with a police report of identity theft are entitled to receive up to 12 free credit reports, one per month for the 12 months following the date of the police report. The procedure for requesting free monthly reports is different for each of the credit bureaus.

Experian: Make a single request to receive all of your free monthly reports. Mail your request for 12 free monthly reports to Experian at P.O. Box 9554, Allen, TX 75013. Enclose a copy of the police report of identity theft, a copy of a government-issued identification card (such as driver's license, state or military ID), and a copy of proof of current mailing address (utility bill, bank or insurance statement showing name, current mailing address, and date of issue). Also provide your full name including middle initial (and generation such as Jr., Sr., II, III), previous addresses for the past two years, Social Security number and date of birth.

TransUnion: Write or call in your request each month. Mail to TransUnion, P. O. Box 6790, Fullerton, CA 92834. Or call the toll-free number printed on your most recent TransUnion credit report. Provide your full name including middle initial (and generation such as Jr., Sr., II, III), Social Security number, date of birth, and proof of residence (such as utility bill or bank statement).

Equifax: Write or call in your request each month. Mail to Equifax Fraud Department, P.O. Box 740250, Atlanta, GA 30374. Or call the toll-free number printed on your most recent Equifax credit report.

Write to creditors

Write a letter to each creditor where an account was opened or used in your name. Repeat what you said in your telephone call. Send a copy of your police report. Black out the account number of any accounts with other creditors on a copy of your completed ID Theft Affidavit and send it. See the Sample Letter to Creditor on Existing Account on page 8 and Sample Letter to Creditor on New Account on page 9.

Consider a Credit Freeze

The strongest protection against new accounts being opened in your name is a credit freeze, also called a security freeze. A freeze means that your file cannot be shared with potential creditors, insurers, employers, or residential landlords without your permission. For more information, see our **CIS 10: How to Freeze Your Credit Files.**

If Your Debit Card or Number is Stolen...

A debit card is an ATM card with a credit card logo on it. It accesses money directly from your bank account, and the legal protections are different from those for credit cards. If your debit card is compromised, call your bank right away and cancel the card. The bank will send you a new debit card and your checking account number will not change. The stolen money, however, will be gone while your bank investigates the matter. If you call the bank within two business days of the fraudulent transaction, your liability is limited to only $50. As time goes by, your liability for fraudulent transactions increases. If you wait more than 60 business days from the date the bank mailed the statement with the fraudulent transaction, you could lose the entire amount of the fraud.

If your checks, ATM card or Bank Account Information Are Lost or Stolen...

Call the bank and close your bank account. Open a new one with a new account number. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses. Report the stolen checks to the check verification companies that retail stores use. You can also contact major check verification companies. Ask them to notify retailers who use their databases not to accept the checks on your closed account. Call TeleCheck at 1-800-710-9898 and Certegy, Inc. at 1-800-437-5120. To find out if the identity thief has passed bad checks in your name, call SCAN at 1-800-262-7771. Follow up by writing to your bank. Send your letter by certified mail, return receipt requested.

If You are Contacted by a Debt Collector...

Tell the debt collector that you are the victim of identity theft. Say that you dispute the validity of the debt. Say that you did not create the debt and are not responsible for it. Send the collector a follow-up letter saying the same things. Include a copy of your police report and of any documents you've received from the creditor. Write in your letter that you are giving notice to a claimant under California Civil Code section 1798.93, subsection (c)(5) that a situation of identity theft exists. Send the letter by certified mail, return receipt requested. If the debt collector is not the original creditor, be sure to send your letter within 30 days of receiving the collector's first written demand for payment.

If your driver's license or DMV-issued ID card is stolen...

Immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license. Then call the toll-free DMV Fraud Hotline at 1-866-658-5758. If the thief is using your license as ID, you may want to change your license number. Ask DMV for an appointment. Take a copy of the police report and copies of bills or other items supporting your claim of fraud. You will also need to prove your identity. Take current documents such as a passport, a certification of citizenship or naturalization, or a U.S. military photo ID. DMV will issue a new license or ID card number when you meet all the requirements.

If Your Mail Was Stolen or Your Address Changed by an Identity Thief...

Notify the Postal Inspector if you think an identity thief has stolen your mail or filed a change of address request in your name. To find the nearest Postal Inspector, look in the white pages of the telephone book for the Post Office listing under United States Government. Or go to the Postal Inspection Service's Web site at www.usps.gov/websites/depart/inspect.

If You Are Wrongly Accused of a Crime Committed by an Identity Thief...

"Criminal identity theft" is a label given to a particular type of identity theft. Criminal identity theft occurs when a suspect in a criminal investigation identifies himself or herself using the identity of another, innocent person. A special database in the California Department of Justice can help victims of this kind of identity theft. See our Consumer Information Sheet 8: How to Use the California Identity Theft Registry - A Guide for Victims of "Criminal" Identity Theft.

If Someone Uses Your Social Security Number to Claim Unemployment Benefits or to Work...

If you suspect that someone else has claimed unemployment benefits using your Social Security number, call the California Employment Development Department's toll-free Fraud Hotline at 1-800-229-6297. For more information, see their Web site at www.edd.ca.gov. Search on the site for "fraud." Sometimes, an identity thief will use someone else's Social Security number to be eligible to work. It's a good idea to check your Social Security earnings record to see if income earned by a thief is being posted to your account. You can get a copy of your earnings record by calling 1-800-772-1213. Or get a Request for Social Security Statement (Form 7004) at www.ssa.gov/online/ssa-7004.html. If you believe a thief is using your Social Security number to work or claim Social Security benefits, call the Social Security Fraud Hotline at 1-800-269-0271. Or report Social Security benefits fraud online at www.ssa.gov/oig/hotline/index.htm.